Release Notes for Cisco ASR 1000 Series, Cisco IOS XE 17.16.x

First Published: 2024-12-22

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

About Cisco ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. The routers are engineered for reliability and performance, with industry-leading advancements in silicon and security to help your business succeed in a digital world that's always on. The Cisco ASR 1000 Series is supported by the Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The series is well suited for enterprises experiencing explosive network traffic and network service providers needing to deliver high-performance services.

Note For more information on the features and specifications of Cisco ASR 1000 Series Routers, refer to the Cisco ASR 1000 Series Routers datasheet.

For information on the End-of-Life and End-of-Sale Announcements for Cisco ASR 1000 Series routers, refer to the ASR 1000 Series End-of-Life and End-of-Sale Notices.

Note Cisco IOS XE 17.16.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE 17.16.x release series.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Changed Hardware Features

There are no new hardware features for this release.

New and Changed Software Features in Cisco IOS XE 17.16.1a

Feature	Description
UTD Container Management for SD-Routing Devices	When Cisco IOS-XE autonomous devices transition to Cisco SD-Routing mode, the Unified Threat Defense (UTD) Container Migration feature ensures that existing container functionalities are preserved. From Cisco IOS XE 17.16.1a you can detect, upgrade, and manage UTD Security Virtual Images through Cisco Catalyst SD-WAN Manager. For devices without pre-existing containers, you can also install and manage UTD images using policy groups.
Configure Source Interface for High Speed Logging	From Cisco IOS XE 17.16.1a, you can configure source interfaces for High-Speed Logging (HSL) and SysLog for security logging in Cisco SD-WAN Manager. You can also enable HSL for your firewall messages, to allow a firewall to log records with minimum impact to packet processing.
Speed Test Enhancement for SD-Routing Devices	From Cisco IOS XE 17.16.1a, Cisco Catalyst SD-WAN Manager enables site-to-site speed tests to measure bandwidth between devices over DMVPN tunnels. These tests check upload speed from the source device to the destination, and measure download speed from destination to the source device.
Disablement of Weak SSH Algorithms	From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security.
Enhanced support for binary tracing	From Cisco IOS XE 17.16.1a onwards, you can retrieve events sent to the IOS process in the binary trace using the **show logging process IOS module nhrp** command, without enabling DMVPN event tracing.
Enhancement to the show cellular 0/x/0 connection command	From Cisco IOS XE 17.16.1a, the output for the show cellular 0/x/0 connection command includes these parameters: • Access Point Name (APN) • Cellular Link Uptime
CUBE Features	
CUBE: Secure Communications Interoperability Protocol (SCIP) support in CUBE	From Cisco IOS XE 17.16.1a onwards, Secure Communication Interoperability Protocol (SCIP) voice and video codec that ensures secure traffic sessions between the endpoints. **Note** Preview Feature Disclaimer: The Secure Communications Interoperability Protocol (SCIP) feature in Cisco IOS XE 17.16.1a release is available in 'preview' mode as it includes limited functionality or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice. Cisco Technical Support provides reasonable effort support for features in preview mode. There is no Service Level Objective (SLO) in response times for features in preview mode; response times may be slow.

Resolved and Open Bugs for Cisco IOS XE 17.16.x

Resolved Bugs for Cisco IOS XE 17.16.1a

Bug ID	Description
CSCwm56800	FIA Trace Packet Decode Displays Incorrect Value for Fragmentation Offset.
CSCwk78018	SD-ROUTING: Yang model does not handle properly default ikev2 authorisation policy.
CSCwm58500	MIP 100 stuck in booting state after ROMMON upgrade using 17.3(1r) rommon file.
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled.
CSCwk42493	Cellular interface in last-resort mode should be admin up, line protocol down .
CSCwm72748	Crash in OMPd Process Crashes Due to Sig-abort When Hitting Pthread Limit.
CSCwm74060	IOSD chasfs task crashes when retrieving platform info.
CSCwk62954	Multiple "match address local interface &lt;int&gt;" not pushed from vmanage under crypto profile.
CSCwk79606	PKI Trustpoint password command only allows encryption type 0 and 7 on all IOS XE platforms.
CSCwj33723	Config not synced between active and 3rd member of stack.
CSCwm48459	Software crash with Critical process vip_confd_startup_sh fault on rp_0_0 (rc=6).
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.
CSCwn29062	Traceback log output on router with "DATACORRUPTION" Error Logs.
CSCwm62981	Router crashes with PKI "revocation-check ocsp none" enabled.
CSCwm70520	LNS router Tracebacks generation.
CSCwm74317	'%CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_CMCA_SUDI.
CSCwm54978	Bender/Fugazi/ASR1K: SIT-SDWAN: Selinux: Subject polaris_iosd_t denials 2024-09-16 06:43:22.
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call.

Open Bugs for Cisco IOS XE 17.16.1a

Bug ID	Description
CSCwn32668	L2 traffic go to blackhole due to mac-route originated from blocked node after power-cycle.

Bug ID	Description
CSCwk56961	SD-WAN: Critical Alarm LED Always On.
CSCwn09185	17.16: Router Traffic loss observed on minimal values with time based policy-map.
CSCwn34457	Post power cycle, unable to login to router due to error Authentication failed.
CSCwn31739	Device crashes when EPC is configured on 100Gb link.
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface.
CSCwn06573	Router crash due to Critical process cpp_cp_svr fault on fp_0_0 (rc=134).
CSCwm71639	cpp_cp_svr crash noticed when configured service-policy to a Dialer interface.
CSCwn24226	GETVPN Mismatch in GMs reported across COOP Due to KEK Sync Issue Between Prim & Sec KSs.
CSCwn40906	Router crash observed when optimizing encrypted traffic with DRE.
CSCwn19586	Certificate-based MACSEC flapping when dot1x reauth timers are set and after reload router.
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed.
CSCwn39447	SpeedTest might work abnormally after changing system-ip.
CSCwn35476	cflowd source interface for sub-interface does not get pushed to cedge.
CSCwn24036	Tx/Rx optical power values diffrent for "show int" and "show hw-module".

ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html.

Note After upgrading the ROMmon to version 17.3(1r), you cannot revert it to a version earlier than 17.3(1r) for the following platforms:

- ASR 1001-HX
- ASR 1002-HX

This restriction is only applicable for these platforms. If you have upgraded to ROMmon version 17.3(1r) on any other platform, reverting to an earlier version of ROMmon is permitted and does not cause any technical issues.

Related Documentation

- Release Notes for Previous Versions of ASR 1000 Series Aggregation Services Routers
- Hardware Guides for Cisco ASR 1000 Series Aggregation Services Routers
- Configuration Guides for ASR 1000 Series Aggregation Services Routers
- Product Landing Page for ASR 1000 Series Aggregation Services Routers
- Datasheet for ASR 1000 Series Aggregation Services Routers
- Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers
- Cisco ASR 1000 Series Aggregation Services Routers ROMmon Upgrade Guide
- Field Notices
- Cisco Bulletins

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

© 2024 Cisco Systems, Inc. All rights reserved.